No. 12-1142

IN THE SUPREME COURT OF THE UNITED STATES

HANNAH JASPER,
PETITIONER/CROSS-RESPONDENT

v.

SPRINGFIELD MUNICIPAL HEALTH CLINICS & WILLIAM DALY,
RESPONDENT/CROSS-PETITIONER

ON WRIT OF CERTIORARI TO THE UNITED STATES
COURT OF APPEALS FOR THE TWELFTH CIRCUIT

BRIEF FOR PETITIONER/CROSS-RESPONDENT HANNAH JASPER

TEAM NO. 2118
Counsel for Petitioner/Cross-Respondent

QUESTIONS PRESENTED

1. Whether the government violates a patient's right to confidentiality when it inadvertently discloses her medical records to an unidentified hacker on two separate occasions.
2. Whether a government official violates an individual's substantive due process right by failing to prevent a disclosure of that individual's patient medical records after having a reasonable opportunity to prevent that disclosure.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

UNITED STATES SUPREME COURT CASES

UNITED STATES COURT OF APPEALS CASES

UNITED STATES DISTRICT COURT CASES

CONSTITUTIONAL PROVISIONS

STATUTES

MISCELLANEOUS

OPINIONS BELOW

The opinion of the United States Court of Appeals for the Twelfth District is unpublished but is reproduced at R. 1-9. The opinion and order of the United States District Court for the District of Illinoza is unpublished but is reproduced at R. 10-22.

STATEMENT OF JURISDICTION

The requirement of a formal statement of jurisdiction has been waived under rule 4(a)(i) of the Official Rules of the National Health Law Moot Court Competition.

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

This case involves questions related to the Fourteenth Amendment's guarantee that "[n]o State shall deprive any person of life, liberty, or property, without due process of law." U.S. Const. amend. XIV.

STATEMENT OF THE CASE

1. The Clinics' Computer Network Breaches

The Springfield Municipal Health Clinics provide both primary and non-emergency healthcare services for its patients. (R. 2.) These services include family planning, monitoring of chronic illness, post-hospital rehabilitation, testing

for sexually-transmitted diseases, and blood and urine exams, as well as less sensitive services such as dental care. (R. 2.)

Between 2008 and 2009, the Clinics suffered three separate computer network attacks. (R. 3, 4.) The first security breach occurred in late 2008 when an unauthorized intruder accessed the Clinics' employee e-mail system through an administrator account. (R. 4.) The Clinics, however, did not become aware of the attack until late 2009. (R. 4.)

On February 2, 2009, the Clinics installed SpaceMed, an electronic health records software program. (R. 3.) This software was designed to manage patient files for authorized users and to secure the private health data against unauthorized intrusions. (R. 3.) The Clinics successfully transferred all patient medical files dating back to January 1, 2003, to SpaceMed. (R. 3.)

Mr. William Daly, the Clinics' Chief Information Technology director since 2007, was responsible for managing and securing the Clinics' patient health data. (R. 2, 3.) In conjunction with the implementation of SpaceMed, Mr. Daly instructed all physicians and staff members to create secure passwords consisting of at least eight characters, including one number and one capital letter. (R. 3.) This password sequence would create over 200 trillion unique strings of eight

characters and could secure the system against potential security breaches for many years. (R. 12.)

Less than two weeks later, on February 14, 2009, an unknown "hactivist," or hacker activist, accessed the Clinics' patient medical records stored on SpaceMed by correctly guessing the system administrator account password. (R. 3, 11.) Rather than implement an eight-character password as Mr. Daly instructed the physicians and staff members to do, Mr. Daly retained the default password, which was simply "password." (R. 3.)

Once on the system administrator account, the hactivist had unrestricted access to all patient medical records, including the capability to modify, copy, and delete the master file of patient records. (R. 3.) Although the hactivist did not alter the medical files, he did reveal the details of the attack to a prominent technology blogger, purportedly in the hope that the Clinics' security would be improved. (R. 3.)

When the hack was made public, the Clinics issued an apology to its patients, and Mr. Daly also changed the administrator account password to "11111." (R. 3-4.) Later, Mr. Daly explained that he created this password because it would be easy for others in the IT department to remember. (R. 4.)

Less than eight months later, on October 17, 2009, the Clinics' computer network was breached for the third time. (R. 3.) An unknown hacker likely used the brute-force method of attack, a method of systematically trying combinations of letters and numbers, to discover the administrator account password. (R. 3, 12.) The hacker downloaded and deleted all files on the Clinics' servers. (R. 4.)

An investigation by an outside data security firm revealed that Mr. Daly forgot to change the administrator password after the installation of SpaceMed. (R. 4.) The firm also determined that the "11111" password was vulnerable to even the most common forms of computer hacking, including password-guessing and brute-force attacks. (R. 12.) The firm concluded that there were "several areas of critical inadequacy" in the Clinics' computer servers. (R. 4.)

2. The District Court Proceedings

The Clinics' patients, including Ms. Hannah Jasper and all others whose medical records were downloaded by the unidentified hacker on October 17, 2009, filed a 42 U.S.C. § 1983 suit against the Clinics and Mr. Daly. (R. 4.) The patients sought injunctive and compensatory relief from the Clinics and Mr. Daly and alleged that their constitutional right to privacy was violated by the government's neglect to protect their sensitive health information. (R. 5.)

The United States District Court for the District of Illinoza granted the defendants' motion for summary judgment, finding that the patients' constitutional right to privacy was not violated. (R. 8-9.) After concluding that the Supreme Court precedent was inapplicable to this case of first impression, the district court adopted the Sixth Circuit's state-created danger test. (R. 8.) Under this test, the patients were required to show that the government's disclosure of their sensitive health information put them at immediate risk to their personal security or other fundamental liberty. (R. 8.) The district court concluded that the patients could not articulate a physical harm that was likely to result from the Clinics' disclosure of their medical records. (R. 8.)

3. The Court of Appeals Proceedings

On appeal, the Twelfth Circuit found that the patients' health records were "the quintessential example of private information deserving protection from unnecessary disclosure." (R. 11.) The court found that the Supreme Court's reasoning in *Whalen*, which found security precautions in place to be dispositive, contravened the state-created danger test as underinclusive, because security precaution would be irrelevant under the Sixth Circuit's approach. (R. 13.) Therefore, the court adopted the balancing test that a majority of the courts of

appeals employ to determine whether a constitutional interest in privacy has been invoked. (R. 13.) The court found that the disclosure "served no compelling public interest whatsoever," and, therefore, the balancing fell in favor of the patients' privacy interest. (R. 14.)

After finding that Ms. Jasper had a constitutional interest in the confidentiality of her medical records, the court determined whether Mr. Daly's failure to install adequate computer security was an egregious act, such that it would violate Ms. Jasper's substantive due process right. (R. 14-15.) The court found that Mr. Daly's conduct was not egregious enough to "shock the contemporary conscience." (R. 16.) Rather, the court reasoned that the ubiquity of computer data breaches have been harmless and should not be constitutionalized. (R. 17.)

SUMMARY OF ARGUMENT

The constitutional right to privacy, or the right to be free from government intrusion, is implicit in the Fourteenth Amendment's concept of personal liberty. The right to privacy encompasses the "individual interest in avoiding disclosure of personal matters." *Whalen v. Roe*, 429 U.S. 589, 599 (1977). This Court has

recognized this right to confidentiality for more than thirty years. Additionally, all but two federal circuits recognize the right to confidentiality.

Personal medical records, which contain information regarding an individual's health, financial well-being, and social security, are entitled protection under this right. This Court recognizes that patients have a reasonable expectation of privacy in the confidentiality of their medical records. Moreover, the courts of appeals, by a broad consensus, recognize that the right to privacy safeguards against nonconsensual disclosures of personal medical information by the government.

This individual interest in non-disclosure of medical records must be balanced against the state's interest in disclosure and the related statutory or regulatory regime in place to prevent unwarranted disclosure. Here, the state posits no rationale for nonconsensually disclosing six years' worth of personal medical records to unidentified hackers on two separate occasions. Further, the statutory and regulatory safeguards in place failed to prevent this unwarranted disclosure of personal medical information. Therefore, the disclosure by the Clinics represents a constitutional violation of the patients' right to privacy.

The court of appeals incorrectly analyzed Ms. Jasper's substantive due

process challenge. In a due process challenge to executive action, the threshold question is whether the government official's conduct "shock[s] the conscience." *County of Sacramento v. Lewis*, 523 US 833, 847 n.8 (1997). There was no need for the court of appeals to analyze whether Mr. Daly's conduct manifested an intent to harm. Rather, because this situation allowed Mr. Daly ample opportunity to reflect and make reasoned and rational decisions, the appellate court should have applied a deliberate indifference standard.

Mr. Daly's deliberately indifferent conduct was so egregious that it shocks the conscience and violates Ms. Jasper's substantive due process rights. First, Mr. Daly knew or should have known of the potential risk of inadvertent disclosure. As the Chief Information Technology director, Mr. Daly knew that implementing a strong password was necessary to protect against inadvertent disclosure of medical files. He demonstrated this knowledge by instructing the Clinics' staff to create lengthy and complex passwords. Second, Mr. Daly failed to implement a secure password despite his awareness of a substantial risk of serious harm that may result from delinquent computer security. Although Mr. Daly instructed the Clinics' staff to create lengthy and complex passwords, he failed to change the default password for the system administrator account. Even after the Clinics'

server was breached and he was on notice that increased security precautions were necessary, Mr. Daly did not take reasonable steps to prevent subsequent disclosures and demonstrated a reckless indifference towards the patients' rights. Thus, his deliberate indifference violated Ms. Jasper's substantive due process right.

ARGUMENT

I. THE PRECEDENTS OF THE SUPREME COURT AND FEDERAL CIRCUITS HAVE ESTABLISHED A CONSTITUTIONAL RIGHT TO THE PRIVACY OF SENSITIVE INFORMATION HELD BY THE GOVERNMENT OR ITS AGENTS.

The right to confidentiality, also known as the right to informational privacy, has stood almost unquestioned since this Court first addressed the issue in 1977. The right to confidentiality exists as an aspect of the right to privacy, which this Court described as the "the most comprehensive of rights and the right most valued by civilized men." *Olmstead v. United States*, 277 U.S. 438, 478 (1928). While this Court has not clearly defined the right to confidentiality, it continues to base its decisions around a belief that an individual's sensitive personal information is constitutionally protected. *See NASA v. Nelson*, 131 S.Ct. 746, 751 (2011); *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 457-58 (1977); *Whalen v. Roe*, 429 U.S. 589, 599 (1977).

Nearly every circuit court has recognized a right to confidentiality. *See Barber v. Overton*, 496 F.3d 449, 454 (6th Cir. 2007); *Tuscon Woman's Clinic v. Eden*, 379 F.3d 531, (9th Cir. 2004); *Greenville Women's Clinic v. Comm'r, S.C. Dep't of Health and Envtl. Control*, 317 F.3d 357, 369 (4th Cir. 2002); *Riley v. St. Louis Cnty. Mo.*, 153 F.3d 627, 631 (8th Cir. 1998); *Sheets v. Salt Lake Cnty.*, 45 F.3d 1383, 1387 (10th Cir. 1995); *Doe v. City of New York*, 15 F.3d 264, 267 (2d Cir. 1994); *Daury v. Smith*, 842 F.2d 9,13 (1st Cir. 1988); *Pesce v. J. Sterling Morton High Sch.*, 830 F.2d 789, 795 (7th Cir. 1987); *Hester v. City of Milledgeville*, 777 F.2d 1492, 1497 (11th Cir. 1985); *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 577 (3d Cir. 1980); *Plante v. Gonzalez*, 575 F.2d 1119, 1132 (5th Cir. 1978). These courts have not embraced a uniform application of the right, but have all relied on the precedent laid down by this Court. This Court was given the opportunity to reverse these circuits in *NASA*, but declined to do so. 131 S.Ct. at 751. Instead, the majority continued to express support for a right to confidentiality in reaching their decision. *Id.*

A. The Supreme Court Has Assumed, Without Question, The Right To Information Privacy For More Than Thirty Years.

The right to privacy is "the most comprehensive of rights and the right most valued by civilized men." *Olmstead v. United States*, 277 U.S. 438, 478

(1928). The right to confidentiality exists as a branch of protected privacy interests devoted to the "individual interest in avoiding disclosure of personal matters." *Whalen v. Roe*, 429 U.S. 589, 599 (1977). There is a recognized threat to an individual's privacy rights "implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files." *Whalen*, 429 U.S. at 605. This proclamation is the first formal recognition of the right to confidentiality. This Court has had multiple opportunities to alter or remove this safeguard of individual liberty but, instead, it has continued to acknowledge this right. *See NASA v. Nelson,* 131 S.Ct. 746, 751 (2011).

Since *Whalen*, this Court has revisited the right to confidentiality twice. *See NASA*, 131 S.Ct. at 751; *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 457 (1977). While neither *Nixon* nor *NASA* resulted in a constitutional violation, the presumption of a constitutionally protected privacy interest for sensitive personal information was left in place. In each case, this Court evinced a belief that the personal papers and medical information deserved protection under the Constitution but were simply too unlikely to be improperly disclosed or abused given the facts. *NASA*, 131 S.Ct. at 756-57; *Nixon*, 433 U.S. at 465. Even a

public figure as visible as the President of the United States is not without protected privacy interests in his personal information. *Nixon*, 433 U.S. at 455.

This Court's consistent use of a right to confidentiality without placing it directly in a holding is not an indication that the right does not exist. Rather, it is a sign of adherence to the canon of avoidance. "If there is one doctrine more deeply rooted than any other in the process of constitutional adjudication, it is that we ought not to pass on questions of constitutionality . . . unless such adjudication is unavoidable." *Spector Motor Serv. v. McLaughlin*, 232 U.S. 101, 105 (1944); *accord Ala. State Fed'n of Labor v. McAdory*, 325 U.S. 450, 461 (1945); *Burton v. United States*, 196 U.S. 283, 295 (1905).

Each time this Court has addressed the right to confidentiality, it has been presented with a situation where the facts showed a state interest and concomitant statutory or regulatory protections strong enough to overcome the intrusion into confidentiality; therefore, the constitutional question never needed to be reached. *NASA*, 131 S.Ct. at 763 ("In light of the protection provided by the Privacy Act's nondisclosure requirement, and because the challenged portions of the forms consist of reasonable inquiries in an employment background check, we conclude that the Government's inquiries do not violate a constitutional right."); *Nixon*, 433

U.S. at 465 ("[Because of] the Act's sensitivity to appellant's legitimate privacy interest . . . [and] the unblemished record of the archivist for discretion . . . we are compelled to agree with the District Court that appellant's privacy claim is without merit."); *Whalen*, 429 U.S. at 605 ("New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy."). Ms. Jasper's case is distinct from these precedents because the state interests and security measures that were dispositive in *Whalen*, *Nixon*, and *NASA* are absent here.

Against this background, Ms. Jasper and the other patients have an interest protected by the right to confidentiality. The information compromised was sensitive medical information, similar to that at issue in *Whalen* and *NASA*. *Whalen*, 429 U.S. at 592; *NASA*, 131 S.Ct. at 753. In addition, the patients' data were compiled and held in a centralized computer database controlled and maintained by the government. Therefore, the patients' information was in the exact circumstance that this Court has found implicitly poses a threat to privacy interests. *Whalen*, 429 U.S. at 605. Further, this case involves actual instances of unwarranted disclosure unlike any other case that has come before this Court. While the individuals in *Whalen*, *Nixon*, and *NASA* were concerned with the

potential for unwarranted disclosure of their information, the Clinics *actually* improperly disclosed patient information on two separate occasions. Thus, the concern expressed in *Whalen* has been realized in the case at hand. To deny Constitutional protection of the patients' personal medical information would be inconsistent with over three decades of precedents and would grant Mr. Daly and the Clinics a safe harbor from the dangers created by their actions.

B. Following Decades of Supreme Court Acquiescence To A Constitutional Right Of Confidentiality, Eleven Circuit Courts Have Held That The Right Exists.

Following the lead of this Court in *Whalen* and *Nixon*, eleven federal appellate courts have recognized a constitutionally protected right to informational privacy. *See Tucson Woman's Clinic v. Eden*, 379 F.3d 531, 551 (9th Cir. 2004); *Greenville Women's Clinic v. Comm'r, S.C. Dept. of Health and Envtl. Control*, 317 F.3d 357 (4th Cir. 2002); *Riley v. St. Louis Cnty. Mo.*, 153 F.3d 627 (8th Cir. 1998); *Sheets v. Salt Lake Cnty.*, 45 F.3d 1383 (10th Cir. 1995); *Doe v. City of New York*, 15 F.3d 264 (2d Cir. 1994); *Daury v. Smith*, 842 F.2d 9 (1st Cir. 1988); *Pesce v. J. Sterling Morton High Sch.*, 830 F.2d 789 (7th Cir. 1987); *Hester v. City of Milledgeville*, 777 F.2d 1492 (11th Cir. 1985); *J.P. v. DeSanti*, 653 F.2d 1080 (6th Cir. 1981); *United States v. Westinghouse Elec.*

Corp., 638 F.2d 570 (3d Cir.1980); *Plante v. Gonzalez*, 575 F.2d 1119 (5th Cir. 1978). A number of these courts have applied the right to confidentiality directly to medical records similar to the patients' files in this case. *See,* e.*g.*, *Tucson Woman's Clinic*, 379 F.3d at 553 (disclosure of abortion providers' medical records); *Greenville Women's Clinic*, 317 F.3d at 369 (disclosure of abortion providers' medical records); *A.L.A. v. West Valley City*, 26 F.3d 989, 990 (10th Cir. 1994) (disclosure of personal medical information); *Doe*, 15 F.3d at 267 (disclosure of HIV status); *Westinghouse*, 638 F.2d at 577 (disclosure of employee medical records). However, the most revealing decision to come from this Court is *NASA*.

Each circuit court that has recognized the right to confidentiality has done so in the wake of *Whalen* but before *NASA*. Accordingly, when *NASA* was decided, the majority could easily have rebuked the lower courts' holdings that there is a right to confidentiality had it felt they were misinterpreting *Whalen* and *Nixon*. It is telling that the majority chose not to do this. Instead of quashing any interest in confidential information, the majority assumed that there was Constitutional protection and proceeded to resolve the case on whether that right had been violated. *NASA*, 131 S.Ct. at 7634-64. Like *Whalen* and *Nixon*, the

majority came to its decision by operating under the assumption that the Constitution protects confidentiality in personal matters, but was able to resolve the case without having to reach the constitutional issue. *Id.*

Although this Court has never explicitly held that a right to confidentiality exists, it has decided cases based around that right for more than three decades. This unquestioned use of the right has led eleven out of thirteen Circuit Courts of Appeals to believe that a right to confidentiality exists. These courts have created precedents that are binding in all fifty states. When this Court decided *NASA*, it expressed no concern or misgivings about the development of the right to confidentiality within the lower courts, but continued to operate under the same assumption it had in *Whalen* and *Nixon*. *NASA*, 131 S.Ct. at 751. If this Court denies Ms. Jasper and the patients protection of their sensitive personal information, it would undo a significant amount of jurisprudence throughout the United States' federal courts.

C. The Constitutional Right To Confidentiality Guarantees Against The Disclosure Of Personal Matters, Including Medical Records And Medical Communications, By The Government Or Its Agents.

The right to confidentiality is the "individual interest in avoiding disclosure of personal matters." *Whalen,* 429 U.S. at 599; *see also Nixon,* 433

U.S. at 457 (reaffirming the existence of a right to privacy of personal matters). "Personal matters" includes, at a minimum, personal medical records. Because "[i]t has long been the Court's 'considered practice not . . . to formulate a rule of constitutional law broader than is required by the precise facts to which it is to be applied," the issues of whether the right to confidentiality applies to other "personal matters" will not be addressed here. *Clinton v. Jones*, 520 U.S. 681, 690 n.11 (1997) (quoting *Ala. State Fed'n of Labor,* 325 U.S. at 461).

By a broad consensus, the courts of appeals understand the right to confidentiality to protect personal medical information. *See, e.g., Anderson v. Romero*, 72 F.3d 518, 522 (7th Cir. 1995) (recognizing the existence of a constitutional right to confidentiality in medical records); *Doe*, 15 F.3d at 267 (asserting that the right to informational privacy includes protection of individual health information); *Westinghouse Elec. Corp.*, 638 F.2d at 577 (finding personal health information is "well within the ambit of materials entitled to privacy protection").

Both the judiciary and legislature have recognized many reasons for defining the right to confidentiality to include personal medical information. Foremost among these is a patient's reasonable expectation of privacy that the

results of diagnostic tests performed in a hospital will remain confidential within the medical community. *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (overturning a policy that allowed law enforcement to compel pregnant drug addicts to undergo treatment in the threat of criminal action). In fact, "an intrusion on that expectation may have adverse consequences because it may deter patients from receiving needed medical care." *Id.* at 78 n.14 (citing *Whalen*, 429 U.S. at 599-600). Even those courts that narrowly define the scope recognize that the right to privacy protects against the disclosure of diagnostic test results, including HIV status. *See, e.g., Herring v. Keenan*, 218 F.3d 1171, 1175 (10th Cir. 2000) (holding that HIV status receives privacy protection from disclosure); *contra Doe v. Wigginton*, 21 F.3d 733, 740 (6th Cir. 1994) (finding prisoners lacked constitutional right to privacy in HIV status).

Additionally, the failure to keep medical records confidential breaches the trust between patients and physicians and diminishes the provision of health care.[1]

> The doctrine of confidentiality is the cornerstone of the physician-patient relationship. Only by being completely candid with a

[1] "The patient whose privacy and sensibilities are safeguarded will be more likely to reveal information that will result in improvement or cure. This benefits the individual and, in turn, the community and, ultimately, the population." *Ruhlmann v. Ulster County Dept. of Soc. Servs*., 234 F. Supp. 2d 140, 182 (N.D.N.Y. 2002).

> physician concerning his or her health history and present symptoms can a patient be assured of receiving the best medical care. In turn, the patient reasonably expects that all confidential information relayed to the physician will not go beyond the physician's office. The genesis of this doctrine can be traced to Hippocrates, widely acknowledged as the father of medicine. . . . [T]he Hippocratic oath, states: ". . . and whatsoever I shall see or hear in the course of my profession . . . if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets. . . ."[2]

Congress recognized the sanctity of patient medical information when, in 1996, it enacted the Health Insurance Portability and Accountability Act (HIPAA), which requires health care providers to ensure the confidentiality of all electronically-stored health records. Social Security Act § 1173, 42 U.S.C. § 1320d-2, 45 C.F.R. § 164.306. This broad recognition of the import of patient health information privacy supports this Court's holding that patients have an expectation of privacy in their medical records. *See Ferguson*, 532 U.S. at 78.

The medical records released by the Clinics falls squarely within the scope of the right to confidentiality. Personal health information pertaining to family planning, monitoring of chronic illness, post-hospital rehabilitation, testing for sexually transmitted diseases, and blood and urine tests was disclosed to an

[2] Kristyn S. Appleby & Joanne Tarver, Med. Records Rev., § 1.7 Confidentiality (2010).

unidentified hacker. Thus, this case presents the question left unanswered in *Whalen*: whether an "unwarranted disclosure of accumulated private data whether intentional or unintentional or by a system that did not contain comparable security provisions" violates the right to information privacy. *Whalen*, 429 U.S. at 605-06.

1. Patients' interest in privacy of their medical records outweighs the government's interest in inadvertently disclosing six years of electronic medical records to an unidentified hacker.

Recognizing the right to information privacy is not absolute, a majority of courts, including this Court, require the government to demonstrate a substantial interest in disclosure of sensitive personal matters, which is balanced against the individual's interest in non-disclosure. The *Whalen* Court weighed the state's "vital interest in controlling the distribution of dangerous [prescription] drugs" against the individual patient's interest in confidentiality in addressing a state statute requiring doctors to provide the state with a copy of every prescription for certain addictive medications. *Whalen*, 429 U.S. at 598-99, 601-02. Finding the state's program was narrowly-tailored and "accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures," this Court held that the statute was constitutional. *Id.* at 601-05; *accord Nixon*, 433 U.S. at 465

(holding the public's interest in the preservation of the presidential papers outweighed President Nixon's expectation of privacy in his personal communications).

Three decades later, this Court applied a similar balancing test in a case challenging the government's collection of personal information for employment purposes. *NASA*, 131 S. Ct. at 759-60. Again, this Court found that the government's compelling interest – here, in evaluating its potential employees for fitness to perform – outweighed the plaintiffs' interest in non-disclosure of their recent illegal drug treatment or counseling. *Id.* at 763-64. In line with the *Whalen* and *Nixon* reasoning, this Court held that a "statutory or regulatory duty" to avoid nonconsensual disclosures provided sufficient protection against the unwarranted disclosure of employee information by the government. *Id.* at 761 (quoting *Whalen*, 429 U.S. at 605).

A majority of lower courts have interpreted *Whalen* and *Nixon* as requiring a balancing of the interests at issue in cases concerning privacy. *See Daury*, 842 F.2d at 13 (finding that the public interest outweighed an underperforming school principal's right to informational privacy); *Doe*, 15 F.3d at 269 (requiring the city's interest in disseminating information to be

"substantial" and balanced against the plaintiff's right to confidentiality); *Plante*, 575 F.2d at 1134 (finding a balancing test proper to evaluate invasion of privacy claims); *Denius v. Dunlap*, 209 F.3d 944, 956 (7th Cir. 2000) (requiring "a sufficiently strong state interest" to overcome the right to confidentiality); *Hester*, 777 F.2d at 1497 (assessing privacy rights by balancing the interests they serve and inhibit). This interpretation most evidently extends from the *Whalen*, *Nixon*, and *NASA* decisions, which each found that the government's interest in collection of information and the statutory safeguards in place to protect against unwarranted disclosures trumped the individual's interest in "avoiding disclosure of personal matters." *See NASA*, 131 S.Ct. at 763-64.; *Nixon*, 433 U.S. at 465; *Whalen*, 429 U.S. at 601-04.

Here, the government presents no rationale for inadvertently disclosing six years of individually-identifiable patient records to an unidentified computer hacker. (R. 13-14.) At best, individually-identifiable health information was inadvertently released by the Clinics as part of a "political hactivist's" statement. (R. 3.) At worse, those files were released to an identity theft or publishing house. Although the object of those files' release is speculative, the fact that the government presents no interest for disclosing them is not.

Conversely, the patients' interest in confidentiality of their medical records, which range from urine and blood results to matters of family planning, likely including contraceptive and abortive services,[3] is beyond question. (R. 3.) *See Ferguson*, 532 U.S. at 78 (finding a reasonable expectation of privacy in the results of diagnostic tests); *Doe v. Delie*, 72 F.3d 1133, 1140 (3d Cir. 2001) (citing *Doe v. Se. Pennsylvania Transp. Auth.*, 72 F.3d 1133, 1140 (3d Cir. 1995) ("It is beyond question that information about one's HIV-positive status is information of the most personal kind and that an individual has an interest in protecting against the dissemination of such information."). Accordingly, Ms. Jasper's individual interest in the confidentiality of her medical records outweighs the state's non-interest in inadvertently revealing that information to an unidentified source.

Furthermore, although HIPAA requires health care providers to "protect against any reasonably anticipated threats or hazards to the security or integrity of [protected health information]," 45 C.F.R. § 164.306, this "concomitant statutory

[3] The Joint Commission, an independent institution that accredits health care providers, requires medical records to contain, among other things, "sufficient information to identify the patient, support the diagnosis, [and] justify treatment, document hospital course and results of treatment." Med. Records Rev. § 1.3 Content.

or regulatory duty" did not prevent government from inadvertently disclosing patient medical records to an unidentified hacker. *See Whalen*, 429 U.S. at 605. Therefore, the balance of interests here weighs heavily in favor of Ms. Jasper and the Clinics' patients.

2. The Sixth Circuit's "state-created danger test" misapplies Supreme Court precedents on the right to information privacy and ignores from important public policy concerns regarding privacy.

The state-created danger test, rejected by the court of appeals in this case, incorrectly interprets Supreme Court precedent and fails to address the important policy principles behind privacy protection and, as such, should not be applied in cases concerning the right to informational privacy. This Court acknowledged that the right to information privacy protects the disclosure of "personal matters" regardless of their relation to other fundamental rights. *See Nixon*, 433 U.S. at 457-58, 462; *Whalen*, 429 U.S. at 599-600. More recently, in assuming a constitutional right to information privacy, this Court in *Nelson* discussed not the duty of state actors but the government's interest in collecting information on its potential employees' past drug use and the extent to which the "personal matters" at issue were protected. *NASA*, 131 S.Ct. at 761-62.

Conversely, the Sixth Circuit recognizes only a narrow corollary to the confidentiality right as it pertains to information relating to one's health, family, children, and other interests protected by substantive due process. *J.P. v. DeSanti*, 653 F.2d 1080, 1089 (6th Cir. 1981). Namely, the Sixth Circuit requires the right to privacy at issue be linked to a right that has been found "fundamental" or "implicit in the ordered concept of liberty." *Id.* at 1090. This theory of the right to privacy is incongruous to this Court's precedents. *See NASA*, 131 S.Ct. at 761-62; *Nixon*, 433 U.S. at 457-58, 462; *Whalen*, 429 U.S. at 599-600.

II. NONCONSENSUAL DISCLOSURE OF INDIVIDUALLY-INDENTIFIABLE HEALTH INFORMATION BY A MUNICIPAL HEALTH CLINIC VIOLATES THE PATIENT'S SUBSTANTIVE DUE PROCESS RIGHTS.

A. The "Shocks-The-Conscience" Test Governs All Substantive Due Process Challenges Based On Egregious Executive Misconduct.

In light of a constitutionally protected privacy interest in health information, the nonconsensual disclosure of Ms. Jasper's medical records violates her right to substantive due process. The Due Process Clause of the Fourteenth Amendment provides that "[n]o State shall…deprive any person of life, liberty, or property, without due process of law." U.S. Const. amend. XIV. A core concept in substantive due process analysis is that individuals are protected

against arbitrary governmental action. *Sacramento v. Lewis,* 523 U.S. 833, 845 (1998). However, a constitutional violation does not arise simply because there is a causal connection between government conduct and a subsequent harm. *Ewolski v. City of Brunswick*, 287 F.3d 492, 510 (6th Cir. 2002). The government must have acted with the requisite culpability. *Id*. In a due process challenge to executive action, the threshold question is whether a government official acted with "egregious official conduct" that "shocks the conscience." *Lewis,* 523 U.S. at 846.

However, determining what shocks the conscience is not precise. At one end of the spectrum, negligent conduct is never sufficient for substantive due process liability. *See Daniels v. Williams*, 474 U.S. 327 (1986). At the other end of the spectrum, behavior intentionally causing harm "most likely rise[s] to the conscience-shocking level." *Lewis,* 523 U.S. at 849. Yet, these are the ends of the spectrum. Whether misconduct falling in the middle range rises to a conscience-shocking level "is a matter for closer calls." *Id*. Therefore, a substantive due process violation turns on the context in which it occurs. *Miller v. City of Philadelphia*, 174 F.3d 368, 375 (3d Cir. 1999). A court must analyze the facts and circumstances of the individual case. *See Ewolski,* 287 F.3d at 510.

B. Where The Situation Affords Officials Time To Deliberate Before Acting, The "Deliberate Indifference" Standard Should Apply To Determine Conscience-Shocking Behavior.

Whether Mr. Daly's misconduct shocks the conscience should be analyzed using the deliberate indifference standard. The intent-to-harm standard is appropriate only where an official does not have the ability to fully consider the risks of his actions. *Miller*, 174 F.3d at 375. In hyper-pressured situations like high-speed police pursuits, "unforeseen circumstances" require "instant judgment" or decisions made "in haste, under pressure, and frequently without the luxury of a second chance." *Lewis*, 523 U.S at 853; *see also*, *Terrell v. Larson*, 396 F.3d 975, 978-81 (8th Cir. 2005) (high-speed responses to emergency situations); *Ziccardi v. Philadelphia*, 288 F.3d 57, 66-67 (3d Cir. 2002) (emergency medical situations); *Medeiros v. O'Connell,* 150 F.3d 164, 169-70 (2d Cir. 1998) (hostage situations). If there is subsequent harm in these exigent circumstances, a court may then inquire into whether the official's intentional acts constituted a constitutional violation.

In contrast, where government officials have an opportunity to reflect and make reasoned and rational decisions, the deliberate indifference standard applies to determine whether conduct shocks the conscience. *Lewis*, 523 U.S. at 851

(1998). A time period as insignificant as six minutes may signify such an opportunity where officers have adequate time to fully consider the potential consequences of their conduct. *Estate of Owensby v. City of Cincinnati*, 414 F.3d 596, 602-03 (6th Cir. 2005); *see also, Terrell*, 371 F.3d at 424 (applying a deliberate indifference standard in a situation where state actors were "afforded a reasonable opportunity to deliberate various alternatives prior to electing a course of action."). These situations often arise where the government owes a special duty of care to those in its charge. *O'Connor v. Pierson*, 426 F.3d 187, 203 (2d Cir. 2005); *see also Lewis*, 523 U.S. at 849-50, n.12 (citing, as an example of deliberate indifference, prison guards who fail to provide for the medical needs of pretrial detainees or provide minimally adequate rehabilitation to personnel at state mental institutions). Where "actual deliberation is practical," an actor's "protracted failure to care" rises to conscience-shocking behavior. *Lewis*, 523 U.S. at 833, 853.

Rejecting any form of egregious behavior, the appellate court asserted that Mr. Daly "did not purposely disclose anything" or "exhibit any malice toward" Ms. Jasper. (R. 16.) However, this analysis is irrelevant as to whether his conduct shocked the conscious. Mr. Daly had two weeks to adjust the default

password before the first medical records hacking occurred. (R. 3.) He then had *more than eight months* to implement a more secure password before the next breach took place. (R. 3.) At no point was Mr. Daly forced to make an instant judgment or make a decision under haste, pressure, or without the luxury of reflection. Instead, he had plenty of opportunity – significantly more than the mere six minutes suitable in *Estate of Owensby* – to consider the consequences and make a rationale choice to implement a secure password. *Estate of Owensby*, 414 F.3d at 602-03. He had the luxury to proceed in a deliberate fashion, much like a prison medical official this Court analogized in *Lewis*. 523 U.S at 849-50, n.12. In this situation, actual deliberation was clearly practical. As a result, analyzing whether Mr. Daly intended to harm Ms. Jasper is not necessary to decide whether his actions shocked the conscience – deliberate indifference is the appropriate standard.

C. Mr. Daly Was Not Only Aware Of The Substantial Risk Of Inadvertent Disclosure, But He Also Failed To Prevent Subsequent Disclosures.

Applying the deliberate indifference standard, Mr. Daly's conduct was so egregious that it shocks the conscious. Deliberate indifference may be equated with "subjective recklessness." *Ewolski,* 287 F.3d at 513. The official either

"knows of and disregards" a potential risk of harm, *Id*. (internal citations omitted) (footnote omitted) (quoting *Farmer v. Brennan,* 511 U.S. 825, 837 (1994)), or fails to act in light of a risk of which the official should have known. *Nicini v. Mora*, 212 F.3d 798, 811 (3d Cir. 2000). In other words, liability under this standard requires two showings. First, the evidence must demonstrate that the official subjectively recognized a substantial risk of harm. *Parrish ex. rel. Lee v. City of Cleveland*, 372 F.3d 294, 302 (4th Cir. 2004). Second, the evidence must show that the official subjectively recognized that his actions were inappropriate given that risk. *Id*.

1. Mr. Daly knew or should have known that failing to implement a secure password creates a substantial risk of disclosure.

Mr. Daly knew that a risk of disclosing private patient medical records existed. This liability attaches where an official is directly exposed to information concerning a potential risk or where circumstantial evidence demonstrates that a risk is "so obvious" the official should have known about it. *Ewolski,* 287 F.3d at 513, n. 7. It also applies where an official is aware, or should be aware, that remedial and preventive measures are inadequate to protect against potential risks. *Kaucher v. County of Bucks*, 455 F.3d 418, 428 (3d Cir. 2006).

There is no doubt that Mr. Daly had actual knowledge of the threat of disclosure. Following SpaceMed's installation, Ms. Jasper's medical records were initially disclosed while the system's default password was merely set as "password." (R. 3.) Mr. Daly could argue he was unaware of the potential harm *before* this first violation. However, subjective fault under deliberate indifference does not require a harmed individual to await a constitutional violation before obtaining relief. *See Farmer,* 511 U.S. at 845. Nevertheless, the evidence in this case refutes any attempt to avoid liability.

Circumstantial evidence can sufficiently demonstrate actual knowledge on the part of an official. *Hamilton v. Leavy*, 117 F.3d 742, 747 (3d Cir. 1997). If evidence reveals that a substantial risk of harm was "longstanding, pervasive, well-documented, or expressly noted" by officials in the past, and the circumstances suggest that the official had been exposed to information concerning the risk, he "must have known" about it. *Farmer,* 511 U.S. at 842-43.

In this case, substantial circumstantial evidence existed so that the potential risk of disclosure was so obvious that Mr. Daly, at the very least, should have known about it. He had been the Chief Information Technology director for two years before the first breach occurred. (R. 2.) In his official capacity, Mr.

Daly managed the Clinics' information systems and the security of the Clinics' patient health data. (R. 3.) Therefore, he should have known that there is enough well-documented evidence indicating that violations in informational security protection are a common threat.[4]

Yet, even before the first disclosure occurred, Mr. Daly knew that adequate security measures were necessary to protect against potential disclosure. He carefully instructed all of the Clinic's physicians and staff about creating passwords that consisted of at least eight characters, including at least one number and upper-case and lower-case letters. (R. 3.) These guidelines produced over 200 trillion unique strings of eight characters– a protection strong enough to resist attacks for years. (R. 12.) Mr. Daly understood that implementing strong security protections was vital in protecting the patients' medical records against the risk of inadvertent disclosure. This obvious risk was later confirmed following the last breach. The affidavits of the parties' expert witnesses, both of whom are computer security experts, indicated that the two hacking attacks are very

[4] For example, as noted by dissent in the court below, even a simple Internet search reveals that, since 2005, there have been more than 700 breaches of health records, affecting over 20 million individual records. *See Chronology of Data Breaches,* Privacy Rights Clearinghouse, http://www.privacyrights.org/data-breach/new (last visited September 15, 2012).

common. (R.11.) The Clinics also "expressly noted" their failure to prevent the violations in an apology letter to their patients. (R. 3.)

The two disclosures of patient records were not the only failures in the Clinics' security system. An outside data security consulting firm found that the Clinics' security systems had *several* areas of critical vulnerability. (R. 4.) This inadequacy led to the disclosure of employee emails, also through an administrator account, three months prior to the second medical records breach. (R. 4.) If the Clinics' had maintained proper security measures, it could argue against liability. *See Kaucher*, 455 F.3d at 428 (refusing to hold that officials operating a correctional facility acted with deliberate indifference in creating unsanitary conditions for its employees where the jail was in substantial compliance with state sanitary standards, which also gave officials reason to believe theirs policies and procedures where adequate to ensure sanitary conditions in the workplace). Here, the Clinics not only failed to maintain sufficient security for its patients but also failed its own employees.

Moreover, following the first disclosure, there is no reason to believe that the system's "11111" password could protect against liability. The Clinics and Mr. Daly should have been aware of the potential risks involved maintaining a

"very weak" and "vulnerable" security protection. (R. 10.) As a result, they should be held liable for inadequate protections. *See Kaucher*, 455 F.3d at 428 (refusing to hold that officials operating a correctional facility acted with deliberate indifference in creating unsanitary conditions for its employees where there was no evidence that, at the time officials made their decisions as to conditions at the jail, they were aware, or should have been aware, that their remedial and preventative measures were inadequate to protect their employees from infections). In fact, the password was so inadequate that it was vulnerable to many forms of attack. (R. 10.) In no way was this preventative measure adequate enough to secure the Ms. Jasper's records from disclosure.

In sum, as the Chief Information Technology Director, Mr. Daly not only knew, but also should have known, of the potential risk for inadvertent disclosure of the patient medical records. Moreover, the longstanding and pervasive instances of breaches in the Clinics' security system demonstrate sufficient circumstantial evidence charging Mr. Daly with actual knowledge of the obvious risk of inadvertent disclosure. Therefore, he had subjective awareness of the risk of inadvertent disclosure.

2. Mr. Daly's failure to implement a more secure password despite an awareness of a substantial risk of

serious harm demonstrated unreasonable and reckless indifference towards the patients' rights.

Mr. Daly demonstrated a conscious disregard of a known risk by not taking reasonable steps to prevent the inadvertent disclosure of patient records. Deliberate indifference requires that a person consciously disregard a substantial risk of harm. *Ziccardi*, 288 F.3d at 66. In this way, once an official knows or should know of a potential risk of harm, he "act[s] or fail[s] to act in a manner demonstrating reckless or callous indifference toward the individual's rights." *Ewolski,* 287 F.3d at 513 (internal quotation marks omitted) (citing *Sperle v. Michigan Dept. of Corrections*, 297 F.3d 483 (6th Cir. 2002)). Only if the official takes reasonable measures to avert a potential harm will he not act with deliberate indifference. *Burrell v. Hampshire County*, 307 F.3d 1, 8 (1st Cir. 2002).

The combination of Mr. Daly's actions and omissions demonstrated a reckless indifference in protecting the patients' records. From the outset, while he was careful to instruct all clinic physicians and staff about creating strong passwords, Mr. Daily failed to change the default password for the system administrator's account. (R. 3.) As a result, the Clinics' data security system easily permitted a breach through the default password "password." (R. 3.) Here, if Mr. Daly found it necessary to instruct other staff members to create strong

passwords, but failed to respond appropriately himself, he was deliberately indifferent to the perceived risk of inadvertent disclosure. *See Parrish ex. rel. Lee v. Cleveland*, 372 F.3d 294 (4th Cir. 2004).

Nevertheless, an official who then knows of a substantial risk of harm may be found free from subsequent liability if he reasonably responds to the risk, even if the harm is ultimately not avoided. *Hamilton*, 117 F.3d at 748 (citing *Farmer*, 511 U.S. at 845). Conceivably, if an official responds "in good faith," his actions may negate deliberate indifference if the response were inadequate from an objective standpoint. *Burrell*, 307 F.3d at 8.

In this case, Mr. Daly did not respond in good faith to ensure that the patients' records were protected against inadvertent disclosure. Following the first disclosure, Mr. Daly changed the system administrator password to "11111". (R. 3.) This protection, however, was very weak and vulnerable to attack. (R. 12.) Thus, it was not surprising that the Clinics' servers allowed a second disclosure to occur. (R. 3.) Mr. Daly later tried explained that, because others in the IT department also use the system administrator account, he wanted to set something easy to remember for the time being, and then come back and set a more secure password when there was more time. (R. 4.) However, his

admission of fault should not be disregarded. (R. 4.) He displayed a "protracted failure to care" and never did change the administrative password. *Lewis*, 523 U.S. at 833, 853. This failure was not a reasonable or good faith response, especially in light of Mr. Daly's awareness that an inadvertent disclosure had occurred previously due to inadequate security protections.

In sum, Mr. Daly consciously disregarded the known risk of inadvertent disclosure. He expressly told the Clinics' physicians and staff to create strong passwords, but failed to create one for the administrative password. As a result of this inadequate security, Ms. Jasper's private patient medical records were disclosed. While he then responded by changing the default password, he failed for a second time to implement a secure password to prevent subsequent harm. His response was clearly not reasonable in light of the circumstances.

D. Mr. Daly Did Not Have a Countervailing Interest That Prevented Him From Taking Reasonable Steps to Protect Against The Risk of Disclosure.

Mr. Daly's failure to prevent disclosure of Ms. Jasper's private patient medical records was not outweighed by any countervailing interest. Acts of deliberate indifference are only justified where some countervailing, mandatory

governmental purpose motivates that conduct. *Hunt v. Sycamore Cnty. Sch. Dist. Bd. of Educ.*, 542 F.3d 529, 543 (6th Cir. 2008).

The deliberate indifference standard incorporates the idea that officials are forced to consider countervailing duties before taking action. *See Farmer*, 511 at 837. Thus, even where a governmental official is subjectively aware of a substantial risk of serious harm, his actions may not constitute deliberate indifference if his conduct is motivated by a countervailing, legitimate governmental purpose. *Hunt*, 542 F.3d at 542. This is true where the actor's countervailing purpose is a mandatory duty imposed by law or the Constitution. *Id*. However, in this case, Mr. Daly acted *contrary to* his affirmative duties.

Mr. Daly had a duty to provide adequate security for personal information in the Clinics' possession. *See Whalen,* 429 U.S. at 605-06. Yet, he failed to implement a more secure password because he wanted "something easy to remember." (R. 4.) This self-serving omission has no legitimate purpose and supports culpability. *See Caldwell v. City of Louisville,* 120 Fed. App'x 566, 576 (6th Cir. 2004). The Clinics also declined to implement a program to lockout users after successive failed attempts to login; in its own words, this would leave their system "vulnerable to 'denial of service' attacks." (R. 12.) However, these

countervailing interests were not constitutionally-imposed or required by law. Even more, these attacks would only *potentially* cause problems in the provision of care by its staff and physicians. (R. 12.)

Mr. Daly also did not have a choice of competing policy interests. At no time did the Clinics mandate that Mr. Daly either choose between following its directors or securing the patient medical records. *Cf. Schroder v. City of Fort Thomas,* 412 F.3d 724 (6th Cir. 2005) (holding the city's failure to enforce a speed limit leading to a child's death was not egregious enough to shock the conscience, where city was obliged to "choose between and among competing policy options"). Moreover, implementing a more secure password would not further harm the patients. *See Ewolski,* 287 F.3d at 510-13 (holding that, even though the police chief was subjectively aware that aggressive intervention in a hostage situation might result in harm to the hostages, he also had reason to believe that delaying could have led to such harm). Even the appellate court recognized that the Clinics and Mr. Daly "should have protected the sensitive health information…better than they did." (R. 16.) Mr. Daly simply acted unreasonably in light of the circumstances and did not have a legitimate purpose.

Thus, neither Mr. Daly nor the Clinics have any countervailing, mandatory purpose in failing to implement more secure passwords that would justify their deliberate indifference. As a result, their deliberate indifference should be held as arbitrary government action that shocks the conscience.

CONCLUSION

For the foregoing reasons, the judgment of the court of appeals regarding the right to confidentiality should be affirmed and the judgment concerning Mr. Daly's violation of substantive due process should be reversed and remanded for further proceedings.

Respectfully submitted,

Team No. 2118
Counsel for Petitioner/Cross-Respondent

Dated: September 27, 2012